UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,213	03/31/2004	Matthew Paul Duggan	AUS920040010US1	7107

34533 7590 05/11/2009

INTERNATIONAL CORP (BLF)
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN, TX 78767-1469

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
05/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,213	DUGGAN ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 2/5/09.

2. Claims 1-28 are pending.

Response to Amendment

3. The amendment to the specification is a clear intent by the Applicants to restrict embodiments of the claim invention to one of the four statutory categories of patentable subject matter. In particular, by eliminating "transmission media" from the portion of the specification that defines examples of a "recording medium for machine-readable information," this amendment is a clearly disavowal of any subject matter directed to a signal claim.

4. Although applicant's amendment to claim 19-28 is directed to a "manufacture" rather than a signal, the claimed invention is still directed to nonstatutory subject matter as outlined below.

Response to Arguments

5. After further consideration of the claims and in view of section 101 requirement for process claims as held in *In re Bilski*, claims 1-9 are newly rejected under 101 as being directed to nonstatutory subject matter.

6. Applicant's arguments with respect to the prior art rejections have been fully considered but are not persuasive.

7. Applicant argues on pgs. 13-14 of the Remarks, that the applied prior art does not suggest the claimed limitations because the primary reference, Dunn, "does not teach or suggest returning to the system entity the security information in the native format of the second security domain as claimed in the present application, that is, returning the same security information transformed into a format required by the second domain." Remarks, pg. 14. However, Applicant does not provide any further explanation what constitutes a "same security information transformed into a format required by the second domain." Rather, Applicant's specification suggests that the limitations in question merely require establishing a trust between two security domains (see Specification, pg. 9), whereby security information native to one security domain is "linked" with security information native to the second security domain. In view of Applicant's disclosure, Dunn suggests such a feature. In col. 9:22-35, Dunn discloses a user having an account in a first security domain and a second security domain, wherein the two security domains are heterogeneous domains and together define a federated system; the invention establishes a trust relationship between the two security domains via an identity broker:

> 8. 1. User A registers his pageA.net and pageB.net identities with the identity broker 206. 2. User A signs in to the pageB.net mail server using the pageA.net authentication ticket. 3. The pageB.net mail server sends a request to an authentication system to confirm the pageA.net identity. 4. The pageB.net mail server finds that it cannot use the pageA.net authentication ticket. 5. The pageB.net mail server sends the pageA.net authentication ticket to the identity broker 206 specified in the authentication ticket. 6. The identity broker 206 reviews the registered identities associated with the pageA.net identity and finds that the pageB.net identity may be used for mail. 7. The identity broker 206 requests the authentication system to authenticate the pageB.net identity.

8. The identity broker 206 returns the pageB.net identity to the pageB.net mail server in an authenticated manner. Col. 9:17-35.

9. Applicant further argues that the secondary reference Bussler in combination with the primary reference Dunn fails to suggest the features of the claimed invention because Bussler only suggest transforming data "in one direction only, from source-side native phase to source-side application phase, from source-side application phase, and so on. But there is no teaching or suggestion in Bussler of any return from the target side to the source side." Remarks, pg. 14. Applicant's argument is not persuasive, because it does not take into consideration the combined teachings of Dunn and Bussler. The question is not whether one reference or the other suggests a claimed feature, but whether the combined teachings of the prior art suggest the limitations in question. Dunn clear teaches "receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain between two security identity broker (Col. 9:17-35; see steps 2 and 3, supra); transforming the security information including a value transformation for mapping a system's entity's identity in the first security domain to another identity in the second security domain (steps 5-6) and returning to the system entity the security information in the native format of the second security domain (steps 7-8). Bussler teaches enabling two or more heterogeneous applications to exchange communications with one another. In particular, Bussler discloses translating a source-side native phase item to a source-side application phase, and then to a common view phase item. The common view phase item is then

translated to a target-side application phase, and finally to a target-side native phase item. Col. 4:3-11. Hence, Dunn as modified by Bussler, suggest an invention where the translation of the user's security data from pageA.net to pageB.net occurs using a multiphase operation from a first domain native format to a canonical format and then to a second domain native format. Dunn's disclosure of returning the translated security identity (steps 7 and 8) back to the second security domain is still relevant in view of the modification by Bussler. Contrary to applicant's arguments that Bussler teaches away from the claimed invention (Remarks, pg. 15), nothing in Bussler suggest that the resulting operation cannot return the transformed data from the target side to the source side. Bussler's invention emphasizes the ability of heterogeneous applications to communicate with one another, rather than defining an invention that requires a strict flow of data from one entity to another. See col. 2:61-65. The key invention in Bussler is not to provide data from one entity to another entity, but to transform data from a first format particular to a first application to another format particular to a second application to enable integration between the heterogeneous applications. Hence, Applicant's conclusion that Bussler "teach[es] directly away from the claimed returning step in the present application," (Remarks, pg. 15) is not persuasive.

10. Finally, Applicant's argument that there is no motivation to combine the teachings of Dunn with Bussler (Remarks, pg. 16-17) is not persuasive. Bussler expressly discloses integrating a multistage transformation of data between heterogeneous applications to disburse the integration over several participants of the communication,

and thereby reducing the complexity of the conversion. Col. 2:30-36. For these reasons, applicant's claimed invention remains rejected under the prior art of record.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 1-9 and 19-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-9 define a method for cross domain security information conversion, including a receiving step, a translating step and a transforming step, a translating step and a returning step. However, none of these steps require a specific machine; although the claims define receiving from a "system entity" security information and returning the transformed security information to the "system entity," the system entity does not implement the steps of the method. Even if a "system entity" implemented the steps of the method, the term "system entity" is broadly defined to include non-machine entities, such as a human; moreover, the steps of the method are broadly recited such that they do not inherently require the use of a particular machine. Finally, there is no transformation of an article or representation of an article (the method only discloses modification of "security information") See In re Bilski, 2007-1130 at 15, ("At present, however, and certainly for the present case, we see no need for such a departure and reaffirm that the machine-or-transformation test, properly applied, is the governing test for determining patent

eligibility of a process under § 101." The Court also points to the Abele case where a dependent process claim was determined to be statutory under 101 but not the independent claim; the dependent claim was a sufficiently specific transformation because it changed "raw data into a particular visual depiction of a physical object on a display"; the transformed object must be "physical objects or substances" or "representative of physical objects or substances," id. at 30 and 32).

13. As per claims 19-28, although the claims on its face are directed to a specific category of 101 subject matter (e.g., a "manufacture"), that does not end the analysis of patent eligibility. The analysis must also consider whether the claimed subject matter falls within a judicially created exception to section 101. It is noted that this claim is distinguished from the invention of *Warmerdam* because the medium of the instant claim does not store any particular data structures, but merely program instructions. The use of a "medium" for storing the broadly recited steps of claims 1-9 would be, in practical effect, a patent on the abstract idea of receiving from a system entity, in a security service, security information in a first native format; translating the security information from a first format to a canonical format, from a canonical format to a second format, and returning to the system entity the security information in the second format. Limiting the claim to part of a system comprising a "computer readable medium" does not add any practical limitation to the scope of the claim. Similar to a field of use limitation in a process claim, the use of a general "computer readable medium" is insufficient to render an otherwise ineligible claim patent eligible. See Bilski, 545 F.3d

at 957. pg. 11. Hence, claims 19-28 would effectively pre-empt the abstract idea of claims 1-9. See also, *Ex parte Mitchell*, Appeal No. 2008-2012 (BPAI 2008).

Claim Rejections - 35 USC § 103

14. Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable under Dunn et al. US 7,428,750 (hereinafter Dunn) in view of Bussler et al. USPN 7,072,898 (hereinafter Bussler).

15. As per claims 1-9, Dunn discloses a method for cross domain security information conversion (Abstract; col. 2:56-59), the method comprising:

a. receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain (19:22-27; fig. 4, reference nos. 408 and 418);

b. transforming the security information using a predefined mapping from a first security domain to a second security domain, including value transformation and mapping a system entity's identity in the first security domain to another identity in the second security domain (19:29-31; fig. 2, reference no. 216);

c. returning to the system entity the security information in the native format of the second security domain (19:32-35; fig. 4, reference no. 416);

d. wherein receiving security information further comprises receiving a request for security information for the second security domain, wherein the

request encapsulates the security information in a native format of a first security domain (19:20-23);

e. wherein the system entity comprises a computer program product entity requesting access to a resource in the second security domain (19:18-21; fig. 4, reference nos. 402, 412 and 416);

f. wherein the system entity comprises a computer program product entity providing access to a resource in the second security domain (19:34-37; fig. 4, reference no. 412).

16. Dunn does not disclose translating the security information to a canonical format for security information, wherein the canonical format is a data format for security information that is standardized for user in data transformations of security information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; translating the transformed security information in the canonical format to a native format of the second security domain; wherein transforming the security information includes structure transformation; wherein translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function; wherein translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function; and expressing the canonical format in XML, whereby security information is translated between the first native format and the second native format via the canonical format via XSL.

17. Bussler discloses an method for exchanging communications between heterogeneous applications wherein data items go through five processes between a source and destination: 1) source-side native phase, 2) source-side application phase, 3) common view phase, 4) target-side application phase, and 5) target-side native phase, whereby the source-side application phase, common view phase and target-side application phase utilize XML to express the data from the source-side application to the target-side application and vice versa. (3:60-4:43; 5:15-7:51) During the source-side native phase, an item is received from a source application in its native form, wherein the syntax, encoding and arrangement is particular to the source application; this item is then converted to an application-independent syntax using "common" syntax such as an XML document. (5:15-67) During the source-side application phase, elements in the application-independent item are rearranged to convert the item into a common view form. (6:1-34) During the common view phase, the all application-specific formatting and encoding are eliminated to generate a canonical format. (6:38-60) The target-side application phase and the target-side native phases are the corresponding reverse phases to transform and translate the canonical format item to the native format item corresponding to the target. (6:64-7:20) Furthermore, XSL is the standard means of defining transformations of an XML file. Moreover, Bussler discloses that the invention overcomes deficiencies of prior inventions, which centralize integration procedures, by disbursing the integration over the several participants of the communication. (See 2:30-36)

18. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the program instructions stored on the computer program product of Dunn when executed to cause the data processing system to carry out the following steps: translating the security information to a canonical format for security information, wherein the canonical format is a data format for security information that is standardized for user in data transformations of security information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; translating the transformed security information in the canonical format to a native format of the second security domain; wherein transforming the security information includes structure transformation; wherein translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function; wherein translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function; and expressing the canonical format in XML, whereby security information is translated between the first native format and the second native format via the canonical format via XSL. One would be motivated to do so to disburse the integration over the several participants of the communication, thereby reducing the complexity of the conversion (Bussler, 2:30-36)

19. Finally, although neither Dunn nor Bussler expressly disclose the first and second native format is expressed in XML, it is notoriously well known for a federation native format to be expressed in XML. For example, SAML is an XML-based standard

for exchanging authentication and authorization data within a federation. Official notice of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time the invention was made for the second native format to be expressed in XML. One would be motivated to do so because SAML is a proven standard for exchanging authentication and authorization data within a federation. The aforementioned cover the limitations of claims 1-9.

20. As per claims 10-18, Dunn discloses a system for cross domain security information conversion (Abstract; col. 2:56-59), the system comprising:

g. Means for receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain (19:22-27; fig. 4, reference nos. 408 and 418);

h. Means for transforming the security information using a predefined mapping from a first security domain to a second security domain, including value transformation and mapping a system entity's identity in the first security domain to another identity in the second security domain (19:29-31; fig. 2, reference no. 216);

i. Means for returning to the system entity the security information in the native format of the second security domain (19:32-35; fig. 4, reference no. 416);

j. wherein receiving security information further comprises receiving a request for security information for the second security domain, wherein the

request encapsulates the security information in a native format of a first security domain (19:20-23);

k. wherein the system entity comprises a computer program product entity requesting access to a resource in the second security domain (19:18-21; fig. 4, reference nos. 402, 412 and 416);

l. wherein the system entity comprises a computer program product entity providing access to a resource in the second security domain (19:34-37; fig. 4, reference no. 412).

21. Dunn does not disclose means for translating the security information to a canonical format for security information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; means for translating the transformed security information in the canonical format to a native format of the second security domain; wherein transforming the security information includes structure transformation; wherein translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function; wherein translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function; and expressing the canonical format in XML, whereby security information is translated between the first native format and the second native format via the canonical format via XSL.

22. Bussler discloses an apparatus for exchanging communications between heterogeneous applications wherein data items go through five processes between a source and destination: 1) source-side native phase, 2) source-side application phase, 3) common view phase, 4) target-side application phase, and 5) target-side native phase, whereby the source-side application phase, common view phase and target-side application phase utilize XML to express the data from the source-side application to the target-side application and vice versa. (3:60-4:43; 5:15-7:51) During the source-side native phase, an item is received from a source application in its native form, wherein the syntax, encoding and arrangement is particular to the source application; this item is then converted to an application-independent syntax using "common" syntax such as an XML document. (5:15-67) During the source-side application phase, elements in the application-independent item are rearranged to convert the item into a common view form. (6:1-34) During the common view phase, the all application-specific formatting and encoding are eliminated to generate a canonical format. (6:38-60) The target-side application phase and the target-side native phases are the corresponding reverse phases to transform and translate the canonical format item to the native format item corresponding to the target. (6:64-7:20) Furthermore, XSL is the standard means of defining transformations of an XML file. Moreover, Bussler discloses that the invention overcomes deficiencies of prior inventions, which centralize integration procedures, by disbursing the integration over the several participants of the communication. (2:30-36)

23. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dunn to further include: means for

translating the security information to a canonical format for security information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; means for translating the transformed security information in the canonical format to a native format of the second security domain; wherein transforming the security information includes structure transformation; wherein translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function; wherein translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function; and expressing the canonical format in XML, whereby security information is translated between the first native format and the second native format via the canonical format via XSL. One would be motivated to do so to disburse the integration over the several participants of the communication, thereby reducing the complexity of the conversion (Bussler, 2:30-36)

24. Finally, although neither Dunn nor Bussler expressly disclose the second native format is expressed in XML, it is notoriously well known for a federation native format to be expressed in XML. For example, SAML is an XML-based standard for exchanging authentication and authorization data within a federation. Official notice of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time the invention was made for the second native format to be expressed in XML. One would be motivated to do so because SAML is a proven standard for exchanging authentication

and authorization data within a federation. The aforementioned cover the limitations of claims 10-18.

25. As per claims 19-28, Dunn discloses a computer program product for cross domain security information conversion (Abstract; col. 2:56-59), the computer program product embodied on a recordable computer-readable medium (3:51-4:14; 16:2-27), the computer program product comprising program instructions, which when installed and executed on a data processing system, are capable of causing the data processing system to carry out the steps of:

m. receiving from a system entity, in a security service, security information in a native format of a first security domain regarding a system entity having an identity in at least one security domain (19:22-27; fig. 4, reference nos. 408 and 418);

n. transforming the security information using a predefined mapping from a first security domain to a second security domain, including value transformation and mapping a system entity's identity in the first security domain to another identity in the second security domain (19:29-31; fig. 2, reference no. 216);

o. returning to the system entity the security information in the native format of the second security domain (19:32-35; fig. 4, reference no. 416);

p. wherein receiving security information further comprises receiving a request for security information for the second security domain, wherein the

request encapsulates the security information in a native format of a first security domain (19:20-23);

q. wherein the system entity comprises a computer program product entity requesting access to a resource in the second security domain (19:18-21; fig. 4, reference nos. 402, 412 and 416);

r. wherein the system entity comprises a computer program product entity providing access to a resource in the second security domain (19:34-37; fig. 4, reference no. 412).

26. Dunn does not disclose translating the security information to a canonical format for security information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; translating the transformed security information in the canonical format to a native format of the second security domain; wherein transforming the security information includes structure transformation; wherein translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function; wherein translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function; and expressing the canonical format in XML, whereby security information is translated between the first native format and the second native format via the canonical format via XSL.

27. Bussler discloses an apparatus for exchanging communications between heterogeneous applications wherein data items go through five processes between a

source and destination: 1) source-side native phase, 2) source-side application phase, 3) common view phase, 4) target-side application phase, and 5) target-side native phase, whereby the source-side application phase, common view phase and target-side application phase utilize XML to express the data from the source-side application to the target-side application and vice versa. (3:60-4:43; 5:15-7:51) During the source-side native phase, an item is received from a source application in its native form, wherein the syntax, encoding and arrangement is particular to the source application; this item is then converted to an application-independent syntax using "common" syntax such as an XML document. (5:15-67) During the source-side application phase, elements in the application-independent item are rearranged to convert the item into a common view form. (6:1-34) During the common view phase, the all application-specific formatting and encoding are eliminated to generate a canonical format. (6:38-60) The target-side application phase and the target-side native phases are the corresponding reverse phases to transform and translate the canonical format item to the native format item corresponding to the target. (6:64-7:20) Furthermore, XSL is the standard means of defining transformations of an XML file. Moreover, Bussler discloses that the invention overcomes deficiencies of prior inventions, which centralize integration procedures, by disbursing the integration over the several participants of the communication. (2:30-36)

28. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the program instructions stored on the computer program product of Dunn when executed to cause the data processing system to carry out the following steps: translating the security information to a canonical format for security

information; wherein transforming the security information includes transforming information in the canonical format using a predefined mapping from the first security domain to a second security domain; translating the transformed security information in the canonical format to a native format of the second security domain; wherein transforming the security information includes structure transformation; wherein translating the security information in a native format of a first security domain to a canonical format comprises a procedural software function; wherein translating the transformed security information in the canonical format to a native format of the second security domain comprises a procedural software function; and expressing the canonical format in XML, whereby security information is translated between the first native format and the second native format via the canonical format via XSL. One would be motivated to do so to disburse the integration over the several participants of the communication, thereby reducing the complexity of the conversion (Bussler, 2:30-36)

29. Finally, although neither Dunn nor Bussler expressly disclose the second native format is expressed in XML, it is notoriously well known for a federation native format to be expressed in XML. For example, SAML is an XML-based standard for exchanging authentication and authorization data within a federation. Official notice of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time the invention was made for the second native format to be expressed in XML. One would be motivated to do so because SAML is a proven standard for exchanging authentication

and authorization data within a federation. The aforementioned cover the limitations of claims 19-28.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432